

Securing your Insecurities on the Web

Netegrity, Inc.

Sumner Blount

Product Manager

sblount@netegrity.com

Netegrity™

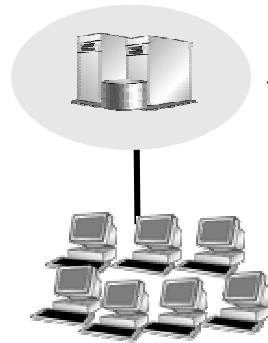


**The leading provider of software &
services for managing and controlling
user access to e-commerce applications**

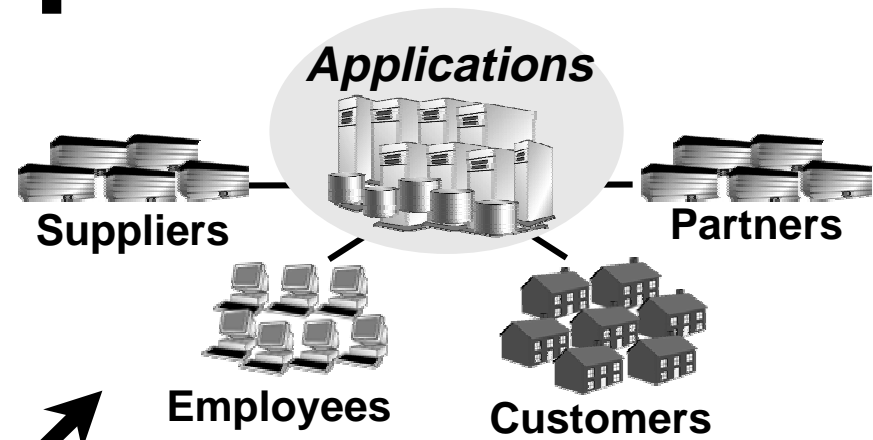
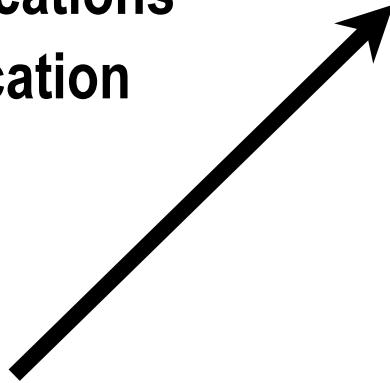
E-commerce Changes Security Requirements

Enterprise Focus

- Restrictive, focused on keeping people out
- Access to few applications
- Local to each application



Employees



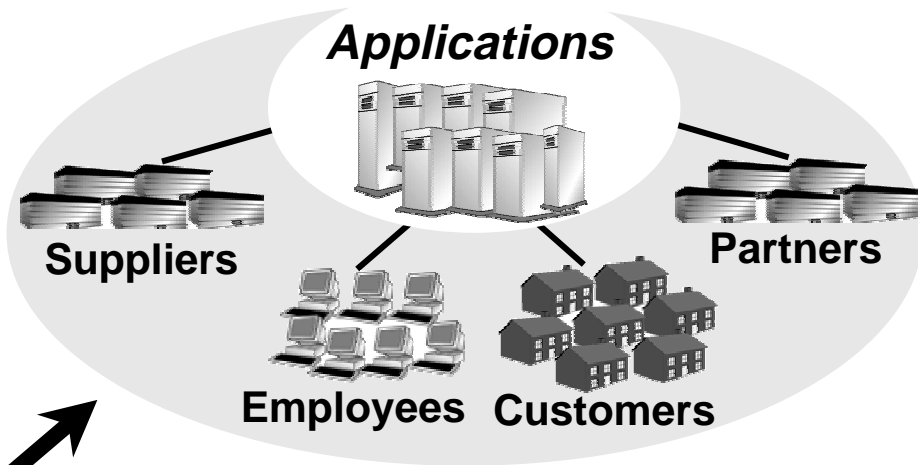
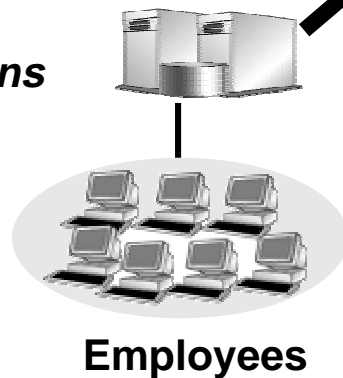
E-commerce focus

- More open, focused on controlling access to information
- Access to many applications
- Centralized on the site

E-commerce Changes Scalability Requirements

Enterprise Focus

- Scales to 10s of thousands
- Accessed by employees only
- IT controls & manages all users



Internet Focus

- Scales to millions
- Accessed by employees, suppliers & customers
- IT controls, but management is distributed

Key Problem: Extranet Privilege Management

- **Extranets must support huge user populations**
- **Developers are re-inventing the access control wheel in every application**
 - **Session management**
 - **Ad hoc policy management**
 - **Single sign-on**
 - **Application-specific Privileges**
- **Privilege change management becomes prohibitively expensive, and essentially insecure, for these large populations**

Requirements: Extranet Privilege Management

- **Shared policy-based entitlement management system external to applications**
- **Centralized control with delegated management**
- **Applications must have easy access to user privilege info**
- **Must allow integration of access control with business logic, for dynamic rule enforcement.**
- **Native integration with directory services**
- **Must scale to huge numbers of user/privilege pairs**

Why Can't Existing Technologies provide this?

■ Web Servers

- Lack of centralized access control
- No sub-page level access control

■ Directories

- Provides an object information namespace, and baseline authentication services
- SSO, personalization need to be custom-built

■ Application Servers

- Cannot manage access across very large user populations
- Access control is different across App. Server platforms

■ PKI

- Provides strong authentication, encryption, and signatures
- Does not provide general-purpose authorization model

Key implementation issues

■ Authentication

- A variety of methods are required
- Auth method should be based on sensitivity of resource
- Re-auth is required if previous authentication was for less sensitive resources

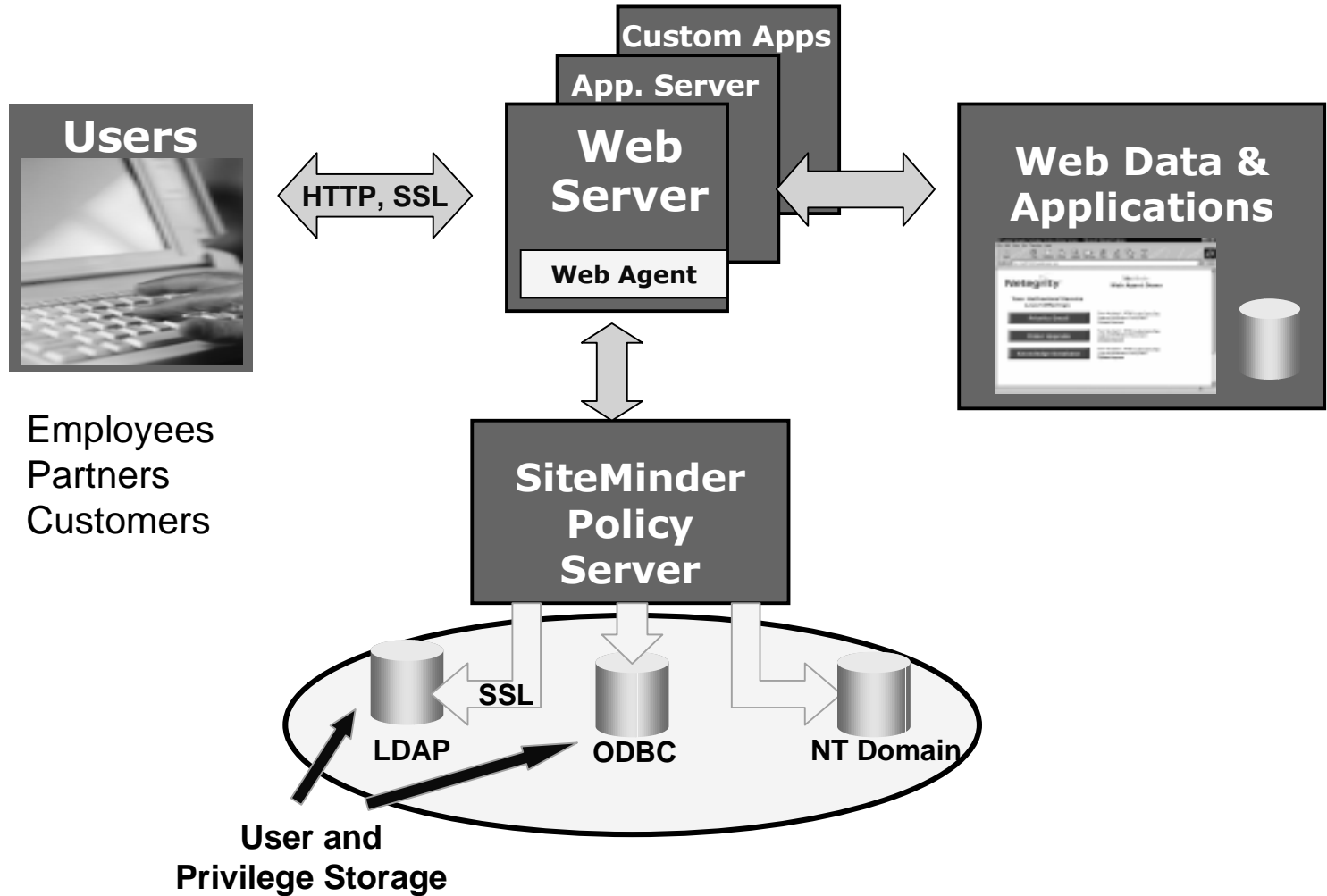
■ Authorization

- Must include variety of author factors (day/time, source, user attributes, etc)
- Integration of business logic with policy enforcement

■ Auditing

- All system/object/user events must be captured
- Viewing of log should be a granular privilege

SiteMinder Architecture



Leveraging the Directory

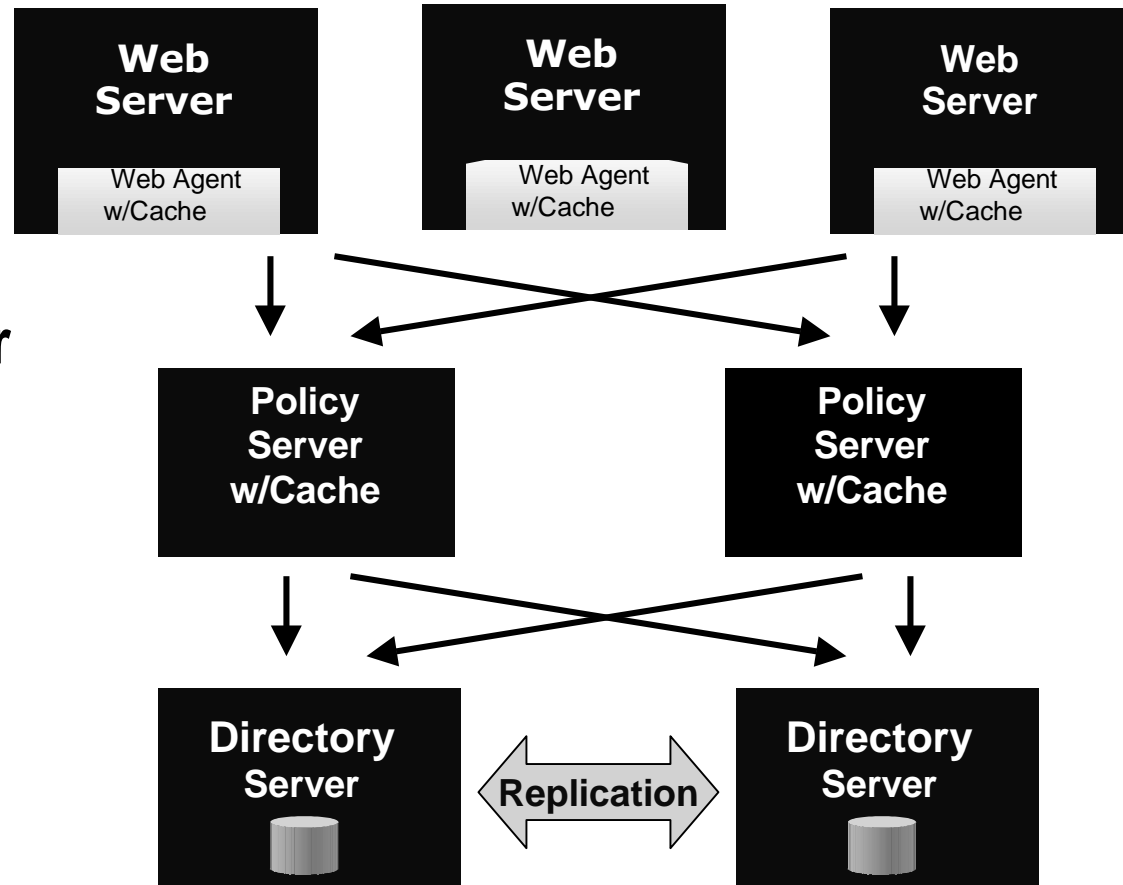
The Directory Service can be used by the PMI to store:

- User credentials and revocation status (CRLs)
- User attributes and profiles
- Access control policies (*not* in separate DB)
- Configuration profiles for security components (for directory-based configuration)

Scalability Design Issues

Key Capabilities

1. Automatic Failover
2. Load Balancing
3. Caches on Agents and Policy Servers



Summary

- **The Extranet market is exploding.**
 - The benefits of extranet deployment can be very profound.
- **Extranets have dramatically different scalability and management requirements than intranets.**
- **A solution specifically tailored for this environment can provide:**
 - Centralized policy management for large numbers of users and policies
 - Single web sign-on
 - Distributed & delegated administration of access control
 - Native integration with directories and PKI